

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-098133

(43)Date of publication of application : 09.04.1999

(51)Int.Cl.

H04L 9/08

G09C 1/00

H04L 9/00

H04N 1/44

(21)Application number : 09-255100

(71)Applicant : MURATA MACH LTD

(22)Date of filing : 19.09.1997

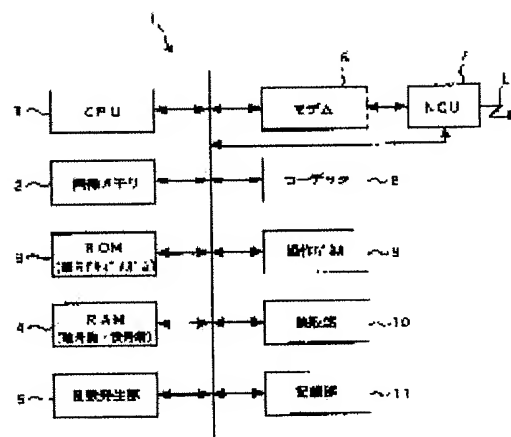
(72)Inventor : HATASHITA MASAHIRO

(54) COMMUNICATION TERMINAL EQUIPMENT AND METHOD FOR CIPHER COMMUNICATION

(57)Abstract:

PROBLEM TO BE SOLVED: To enable simple change of set data and execute secret key mode cipher communication by providing a facsimile equipment with a means for deciphering a 2nd secret key with a 1st secret key and a public key and a means for ciphering data with the deciphered 2nd secret key and transmitting the result.

SOLUTION: The facsimile equipment F is provided with a means for generating a secret key and a public key, a means for transmitting the generated public key, a means for receiving ciphered data by the transmitted public key, and a means for deciphering the ciphered data by the secret key. These means are constituted when CPU 1 executes public key mode cipher algorithm stored in a ROM 3. Namely the CPU 1 generates the 1st secret key and the public key and transmits the generated disclosed key. Then the CPU 1 controls processing for receiving the 2nd secret key ciphered by the public key and deciphering the 2nd secret key by the 1st secret key. In addition, the CPU 1 ciphers data by the deciphered 2nd secret key and transmits the ciphered data.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision
of rejection]

[Date of requesting appeal against examiner's
decision of rejection]

[Date of extinction of right]

(19)日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(11)特許出願公開番号

特開平11-98133

(43)公開日 平成11年(1999) 4月9日

(51)Int.Cl. ⁸	識別記号	F I		
H 0 4 L 9/08		H 0 4 L 9/00	6 0 1 A	
G 0 9 C 1/00	6 6 0	G 0 9 C 1/00	6 6 0 G	
H 0 4 L 9/00		H 0 4 N 1/44		
H 0 4 N 1/44		H 0 4 L 9/00		
			6 0 1 E	
		審査請求 未請求 請求項の数3 O L (全 7 頁)		

(21)出願番号 特願平9-255100

(22)出願日 平成9年(1997) 9月19日

(71)出願人 000006297

村田機械株式会社

京都府京都市南区吉祥院南落合町3番地

(72)発明者 畑下 真広

京都市伏見区竹田向代町136番地 村田機

械株式会社本社工場内

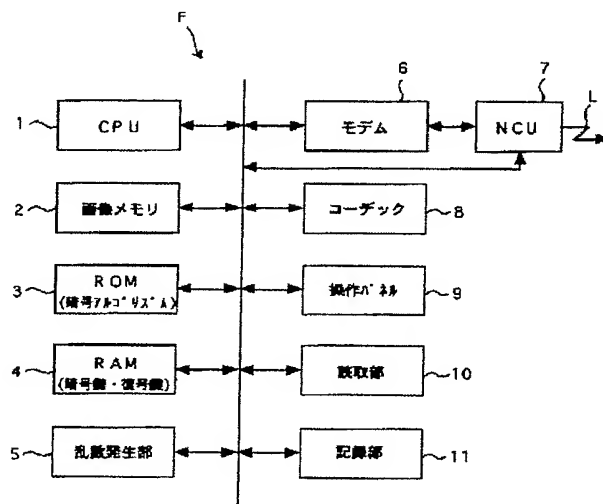
(74)代理人 弁理士 中井 宏行

(54)【発明の名称】 通信端末装置及び暗号通信方法

(57)【要約】

【課題】 簡易に設定データを変更できるようにして、秘密鍵方式の暗号通信ができるようにする。

【解決手段】 乱数発生手段5と、この乱数発生手段5が発生させた乱数に基づいて第1秘密鍵と公開鍵とを生成する手段と、この生成した公開鍵を送信する手段と、この送信した公開鍵により暗号化された第2秘密鍵を受信する手段と、この暗号化された第2秘密鍵を第1秘密鍵と公開鍵により復号化する手段と、この復号化した第2秘密鍵によりデータを暗号化して送信する手段とを備える。



【特許請求の範囲】

【請求項 1】乱数発生手段と、この乱数発生手段が発生させた乱数に基づいて第 1 秘密鍵と公開鍵とを生成する手段と、この生成した公開鍵を送信する手段と、この送信した公開鍵により暗号化された第 2 秘密鍵を受信する手段と、この暗号化された第 2 秘密鍵を上記第 1 秘密鍵と公開鍵により復号化する手段と、この復号化した第 2 秘密鍵によりデータを暗号化して送信する手段とを備えた通信端末装置。

【請求項 2】予め第 2 秘密鍵を設定する手段と、上記公開鍵を受信する手段と、この受信した公開鍵により上記第 2 秘密鍵を暗号化して送信する手段と、この暗号化した第 2 秘密鍵が復号化され、この復号化された第 2 秘密鍵により暗号化されたデータを受信する手段と、この受信したデータを上記第 2 秘密鍵により復号化する手段とを、更に備えた請求項 1 に記載の通信端末装置。

【請求項 3】送信側は、乱数に基づいて第 1 秘密鍵と公開鍵とを生成し、送信した公開鍵により暗号化された第 2 秘密鍵を受信すると、復号化した第 2 秘密鍵によりデータを暗号化して送信する一方、受信側は、上記公開鍵により暗号化して送信した第 2 秘密鍵に基づいて暗号化されたデータを受信すると、このデータを第 2 秘密鍵により復号化することを特徴とする暗号通信方法。

【発明の詳細な説明】**【0001】**

【発明の属する技術分野】本発明は、ファクシミリ装置などの通信端末装置及びこの装置で使用される暗号通信方法に関する。

【0002】

【従来の技術】従来から、ファクシミリ装置などの通信端末装置では、情報セキュリティ対策の一環として暗号通信が行われている。この暗号通信の方法は、暗号アルゴリズムを公開し、多数の者が利用できるようにしているものが主流であり、このアルゴリズム公開型暗号方式には、暗号鍵と復号鍵を同じにしてその両方を秘密にする秘密鍵方式と、暗号鍵と復号鍵を異なるものにして、暗号鍵は公開し復号鍵は秘密にする公開鍵方式とがある。

【0003】秘密鍵方式には DES や FEAL などの暗号方式があり、公開鍵方式には RSA などの暗号方式がよく用いられている。なお、秘密鍵方式は、公開鍵方式に比べて処理速度が速いという特長があるため、データ量が多い場合には特に有効に利用されている。具体的には、秘密鍵方式の場合、データの送信側と受信側の各々に、予め同じ鍵を設定しておく単純な方法以外に、一方（受信側）だけに秘密鍵を設定すればよいために、前もって、公開鍵方式を用いて、送信側から公開鍵を送信し、これによって受信側が秘密鍵自身を暗号化して送信側に返信する方法がある。送信側では、返信された秘密鍵を復号できるので、以降、これを用いて暗号化したデ

ータを送信する。

【0004】なお、この方法においても、送信側が公開鍵を所定のデータの中から任意に設定して送信し、これを基にして受信側が秘密鍵を暗号化する方法と、さらに受信側が秘密鍵を任意に設定しておき、送信側から公開鍵を受信すると、これを基に秘密鍵を暗号化する方法とに分類される。

【0005】

【発明が解決しようとする課題】ところが、上記従来の通信端末装置では、秘密鍵方式の暗号通信において、受信側のみに予め秘密鍵を設定しておく場合でも、その秘密鍵自身の暗号通信の安全性を保つためには、送信側あるいは受信側の設定データを、定期的にキー操作などで設定しなおす必要があり、面倒であった。

【0006】本発明はこのような事情に鑑みて提案されたものであり、簡易に設定データを変更できるようにして、秘密鍵方式の暗号通信ができるようにした通信端末装置及びその暗号通信方法を提供することを目的としている。

【0007】

【課題を解決するための手段】上記目的を達成するために提案される請求項 1 に記載の通信端末装置は、乱数発生手段と、この乱数発生手段が発生させた乱数に基づいて第 1 秘密鍵と公開鍵とを生成する手段と、この生成した公開鍵を送信する手段と、この送信した公開鍵により暗号化された第 2 秘密鍵を受信する手段と、この暗号化された第 2 秘密鍵を第 1 秘密鍵と公開鍵により復号化する手段と、この復号化した第 2 秘密鍵によりデータを暗号化して送信する手段とを備える。

【0008】請求項 1 では、データの送信側となる通信端末装置について提案しており、乱数に基づいて、第 1 秘密鍵と公開鍵を生成するところに特徴がある。この公開鍵は、受信側の第 2 秘密鍵自身を暗号化させるためのものであり、公開鍵を生成したときは、同時に第 1 秘密鍵も生成されているので、暗号化された第 2 秘密鍵を受信すると、これを復号化できる。これによって、第 2 秘密鍵を以降のデータ送信時の暗号化に用いることができる。

【0009】請求項 2 では、請求項 1 の構成に加えて、更に、予め第 2 秘密鍵を設定する手段と、公開鍵を受信する手段と、この受信した公開鍵により第 2 秘密鍵を暗号化して送信する手段と、この暗号化した第 2 秘密鍵が復号化され、この復号化された第 2 秘密鍵により暗号化されたデータを受信する手段と、この受信したデータを第 2 秘密鍵により復号化する手段とを備える。

【0010】すなわち、請求項 2 では、データの受信側となる場合を含めた通信端末装置について提案しており、公開鍵を受信すると、これを用いて第 2 秘密鍵を暗号化し送信する。すると、第 2 秘密鍵で暗号化されたデータを受信するので、このデータを第 2 秘密鍵により復

号化すればよい。請求項3では、請求項1及び請求項2に記載の通信端末装置が使用する暗号通信方法について提案しており、送信側は、乱数に基づいて第1秘密鍵と公開鍵とを生成し、送信した公開鍵により暗号化された第2秘密鍵を受信すると、復号化した第2秘密鍵によりデータを暗号化して送信する一方、受信側は、公開鍵により暗号化して送信した第2秘密鍵に基づいて暗号化されたデータを受信すると、このデータを第2秘密鍵により復号化することを特徴とする。

【0011】

【発明の実施の形態】以下に、図面を参照して本発明の実施の形態を説明する。図1は、本発明の通信端末装置の構成の一例を示すブロック図である。ここでは、通信端末装置の例としてファクシミリ装置Fの構成例を示すが、本発明はこれに限定されることはなく、データの暗号通信機能を備えたパーソナルコンピュータ等であってもよい。

【0012】CPU1はこのファクシミリ装置Fの各部を制御する。画像メモリ2はDRAM等で構成され、送受するファクシミリ通信データを一時記憶する。ROM3は、公開鍵方式のDESやFEALなどや、秘密鍵方式のRSAなどの公開されている暗号アルゴリズムを記憶する他、このファクシミリ装置Fの動作に必要な制御プログラムなどを記憶する。RAM4は処理の実行時に発生する一時的なデータを記憶する。乱数発生部5は、本発明の乱数発生手段を構成し、これによって発生した乱数に基づいて、公開鍵方式の暗号通信を行うべく、秘密鍵（第1秘密鍵）と公開鍵とを生成する（後述）。

【0013】モデム6はファクシミリ通信のために信号の変調、復調を行う。NCU7は通信回線L1（アナログ回線）の閉結、開放を行う。なお、デジタル回線を接続する場合は、モデム6及びNCU7の代わりに、DSUに接続するためのISDNインターフェースなどを備える。コーデック8はMHやMR符号などのファクシミリ通信データに符号化又は復号化する。

【0014】操作パネル9は、このファクシミリ装置Fの動作状態などを表示する液晶表示装置などの表示手段と、このファクシミリ装置Fに対し各種入力設定を各種キーなどの操作手段とで構成される。読取部10は、原稿から画像を読み取りイメージデータにする。記録部11はプリンタで構成され、他のファクシミリ装置などから受信したデータなどをイメージデータにして記録（印字出力）する。

【0015】このファクシミリ装置Fは、更に、公開鍵方式の暗号通信を実行すべく、秘密鍵と公開鍵とを生成する手段と、この生成した公開鍵を送信する手段と、この送信した公開鍵により暗号化されたデータを受信する手段と、この暗号化されたデータを秘密鍵により復号化する手段とを備えている、本発明では、この暗号化されるデータが、以降に説明する秘密鍵方式の暗号通信を実

現するための秘密鍵自身になっているため、このデータとなる秘密鍵を第2秘密鍵と呼び、上記公開鍵方式の秘密鍵を第1秘密鍵と呼ぶことにする。

【0016】なお、上記した各手段は、ROM3に記憶された公開鍵方式の暗号アルゴリズムを、CPU1が実行することによって構成されている。つまり、CPU1は、第1秘密鍵と公開鍵とを生成し、この生成した公開鍵を送信し、この送信した公開鍵により暗号化された第2秘密鍵を受信し、この暗号化された第2秘密鍵を第1秘密鍵により復号化する処理を制御する。

【0017】また、このファクシミリ装置Fは、上述したように、秘密鍵方式の暗号通信を実行すべく、復号化した第2秘密鍵によりファクシミリデータを暗号化して送信する手段を備える。この手段は、ROM3に記憶された秘密鍵方式の暗号アルゴリズムを、CPU1が実行することによって構成される。なお、このファクシミリデータを送信するときの暗号方式には、上記第2暗号鍵の暗号方式と同じあるいは異なる公開鍵方式を用いることもできるが、データ量が多くなるにつれて、処理速度が遅くなることを防ぐため、秘密鍵方式を用いることが好ましい。

【0018】本発明では、乱数発生部5が発生させた乱数に基づいて、第1秘密鍵と公開鍵を生成するところに特徴がある。これによって、いちいち操作パネル9を操作して、これらの鍵のデータを設定する必要がなくなる。以上には、このファクシミリ装置Fが暗号通信の送信側になる場合について説明したが、受信側になる場合は、更に、予め第2秘密鍵を設定する手段としてRAM4を備え、公開鍵方式の暗号通信を実行すべく、公開鍵を受信する手段と、この受信した公開鍵により第2秘密鍵を暗号化して送信する手段とを備える。

【0019】これら通信の手段は、上記送信側となる場合と同様に、ROM3に記憶された公開鍵方式の暗号アルゴリズムを、CPU1が実行することによって構成される。つまり、CPU1は、公開鍵を受信し、この受信した公開鍵により暗号化した第2秘密鍵を送信する処理を制御する。また、このファクシミリ装置Fは、秘密鍵方式の暗号通信を実行すべく、暗号化した第2秘密鍵が復号化され、この復号化された第2秘密鍵により暗号化されたデータを受信する手段と、この受信したデータを第2秘密鍵により復号化する手段とを備える。これらの手段は、ROM3に記憶された秘密鍵方式の暗号アルゴリズムを、CPU1が実行することによって構成される。つまり、CPU1は、第2秘密鍵により暗号化されたデータを受信し、この受信したデータを第2秘密鍵により復号化する処理を制御する。

【0020】図2には、上記した暗号通信方法を具体的に示している。ここでは、公開鍵方式としてRSA暗号方式を使用する場合を示している。RSA暗号方式を説明すると、まず、十分大きな2つの素数pとqを定め、

【数1】

$$n=pq$$

とする。

【0021】次いで、 $(p-1)(q-1)$ と互いに素な正数 e を定める。すなわち、

【数2】

$$(e, (p-1)(q-1))=1$$

である。本発明では、 p 、 q 、 e といった素数が、乱数によって定められることになる。【0022】そして、 $(p-1)(q-1)$ を法とする10
ときの e の逆数 d 、すなわち、

【数3】

$$ed \equiv 1 \pmod{(p-1)(q-1)}$$

を満たす d を求めておく。【0023】そして、公開鍵を n と e 、秘密鍵（本発明の第1秘密鍵）を p と q と d とし、平文 M に対し、

【数4】

$$C \equiv M^e \pmod{n}$$

として暗号文 C を生成する。

【0024】これを、復号化するときには、

【数5】

$$M \equiv C^d \pmod{n}$$

を用いて平文 M を求めればよい。【0025】例えば、公開鍵を $n=55$ 、 $e=7$ とし、秘密鍵を $p=5$ 、 $q=11$ 、 $d=23$ （ $7 \times 23 \bmod 40=1$ ）、平文を $M=3$ とすれば、暗号文は $C=42$ （ $3^7 \bmod 55=42$ ）となり、また、 $42^{23} \bmod 55=3$ （ $=M$ ）によって復号できることになる。【0026】送信側では、乱数に基づき、数式1~3を用いて、第1秘密鍵 p 、 q 、 d と公開鍵 e 、 n とを生成し①、公開鍵 e 、 n を送信する。これに対し、受信側は、数式4を用いて、公開鍵 e 、 n により第2秘密鍵 K （数式4、5では平文 M に相当）を暗号化して秘密鍵 C として②、送信する。送信側は、暗号化された第2秘密鍵 C を受信すると、数式5を用いて第1秘密鍵 d と公開鍵 n により復号化し③、この復号化した第2秘密鍵 K によりデータを暗号化して送信して④、これを受信側は第2秘密鍵 K により復号化する⑤。【0027】次に、このときのファクシミリ装置Fの動作を図3と図4にフローチャートで示す。図3はデータ送信時の動作を示している。CPU1は、操作パネル9によって送信操作がなされると、乱数発生部5で発生させた乱数を基に第1秘密鍵と公開鍵を生成し、これらをRAM4に記憶しておく。そして、公開鍵を送信した後
40 に受信したデータ（暗号化された第2秘密鍵）を、RAM4に記憶しておいた鍵で復号化する。その後は、読取部10で読み取り、コーデック8で符号化して、一旦画像メモリ2に蓄積したファクシミリデータ（符号化データ）を、順次、復号化したデータ（第2暗号鍵）を用いて暗号化し、モデム6とNCU7を介して回線Lに対し
50

て送信する（以上、100~105）。

【0028】一方、図4はデータ受信時の動作を示している。CPU1は、公開鍵を受信すると、予めRAM4に記憶している第2秘密鍵を暗号化して送信する。すると、暗号化されたファクシミリデータ（符号化データ）が、回線Lを通じて送信されて来るので、順次、画像メモリ2に蓄積し、RAM4に記憶している第2秘密鍵を用いて復号化しながら、コーデック8で復号化し、記録部11によって印字出力する（以上、200~204）。

【0029】なお、以上には、送信側で第1秘密鍵と公開鍵とを乱数に基づいて生成する場合を説明したが、さらに受信側で第2秘密鍵を乱数に基づいて生成するようにしてもよい。また、第2暗号鍵の暗号化及び復号化と、ファクシミリデータの暗号化及び復号化とは、同一の演算手段であるCPU1で行うことには限定されず、それぞれ別々の回路を用いて行うようにしてもよい。

【0030】

【発明の効果】以上の説明からも理解できるように、本発明の請求項1に記載の通信端末装置は、乱数に基づいて第1秘密鍵と公開鍵とを生成し、公開鍵を送信して、暗号化された第2秘密鍵を受信する。そして、この第2秘密鍵を第1秘密鍵と公開鍵により復号化して、以降、この復号化した第2秘密鍵によりデータを暗号化して送信する。

【0031】この通信端末装置では、乱数に基づいて第1秘密鍵と公開鍵を生成することができるので、いちいち操作パネルなどを操作して、これらの鍵のデータを設定する必要がなく、秘密鍵方式の暗号通信に用いる秘密鍵自身の暗号通信の安全性を保つことができる。請求項2では、乱数に基づいて生成された公開鍵を受信すると、この公開鍵により第2秘密鍵を暗号化して返信する。すると、第2秘密鍵で暗号化されたデータを受信するので、このデータを第2秘密鍵により復号化すればよい。したがって、予め第2秘密鍵を設定しておけば、これを定期的に設定し直さなくても、秘密鍵方式の暗号通信の安全性を保つことができる。

【0032】請求項3に記載の暗号通信方法では、送信側は、乱数に基づいて第1秘密鍵と公開鍵とを生成し、一方の受信側は、受信した公開鍵により、秘密鍵方式の暗号通信に使用する秘密鍵自身を暗号化して送信側に返信する。これによって、送信側と受信側のいずれにおいても、意識的に設定データを変更することなく、簡単に安全性が高い暗号通信を実施できるようになる。

【図面の簡単な説明】

【図1】本発明に係る通信端末装置の構成の一例を示したブロック図である。

【図2】本発明に係る暗号通信方法の一例を示した図である。

【図3】本発明に係る通信端末装置のデータ送信時の動

7

作の一例を示したフローチャートである。

【図4】本発明に係る通信端末装置のデータ受信時の動作の一例を示したフローチャートである。

【符号の説明】

F・・・ファクシミリ装置

* 1・・・CPU

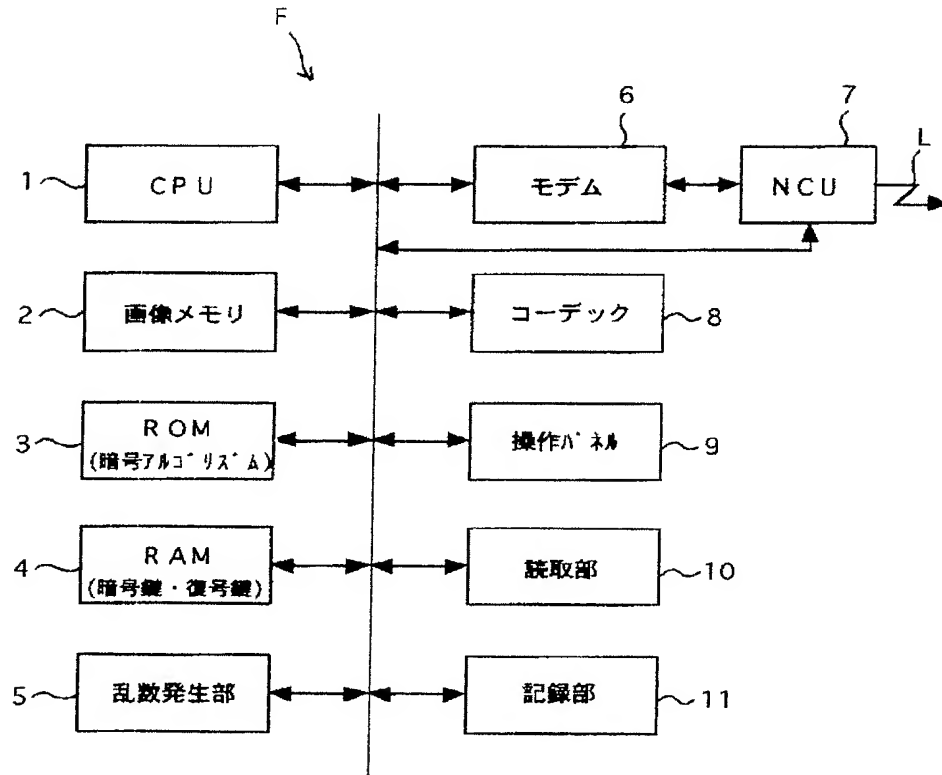
3・・・ROM

4・・・RAM

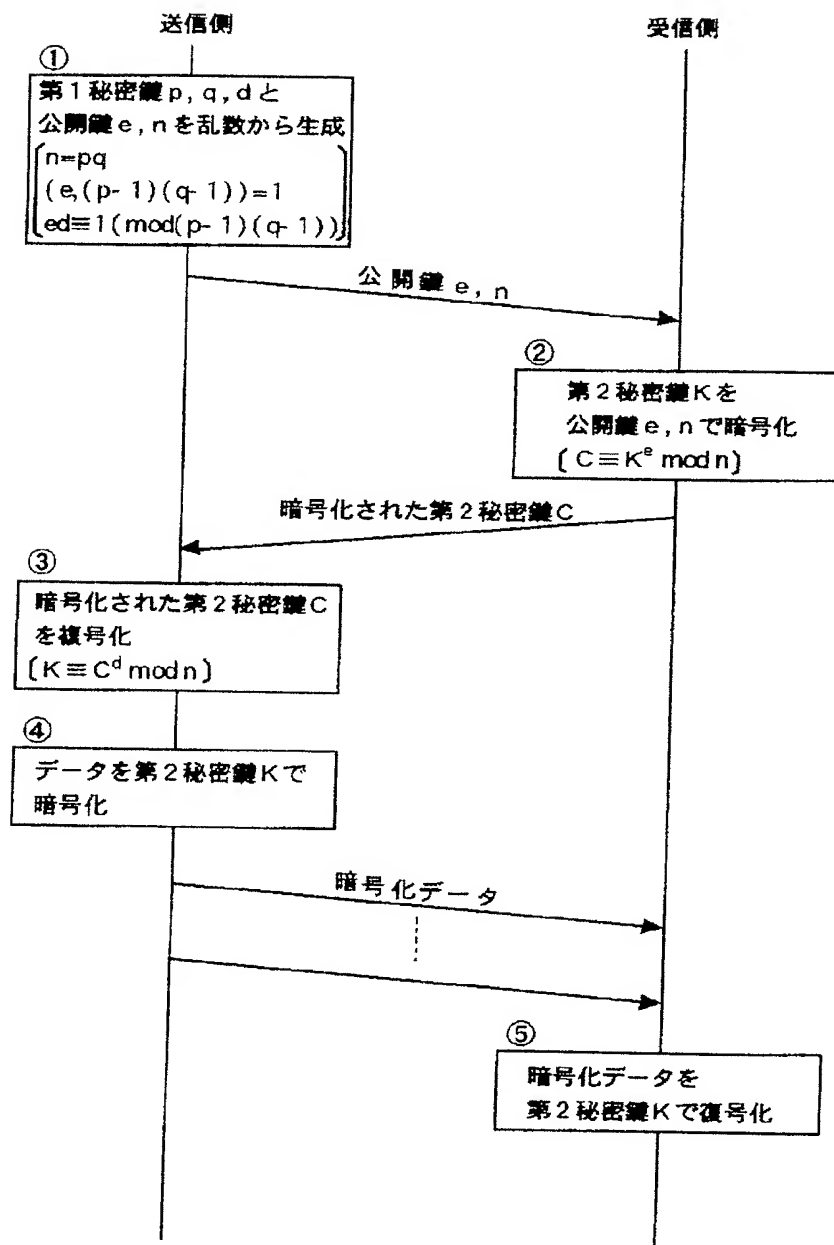
5・・・乱数発生部

*

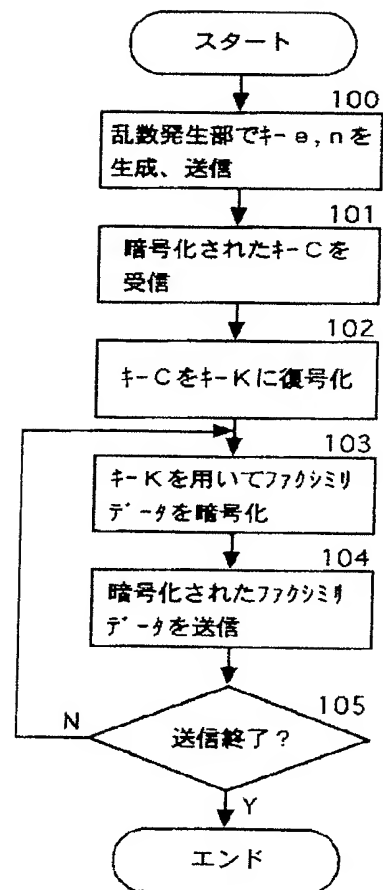
【図1】



【図2】



【図3】



【図4】

